U.S. Department of Justice

Michael J. Sullivan
United States Attorney
District of Massachusetts

Press Office: (617) 748-3139

John Joseph Moakley United States Courthouse
1 Courthouse Way
Suite 9200
Boston, Massachusetts 02210

September 8, 2005

PRESS RELEASE

MASSACHUSETTS TEEN CONVICTED FOR HACKING INTO INTERNET AND TELEPHONE SERVICE PROVIDERS AND MAKING BOMB THREATS TO HIGH SCHOOLS IN MASSACHUSETTS AND FLORIDA

Boston, MA... A Massachusetts juvenile pled guilty in federal court and was sentenced today in connection with a series of hacking incidents into Internet and telephone service providers; the theft of an individual's personal information and the posting of it on the Internet; and making bomb threats to high schools in Florida and Massachusetts; all of which took place over a fifteen month period. Victims of the Juvenile's conduct have suffered a total of approximately $1 million in damages.

United States Attorney Michael J. Sullivan for the District of Massachusetts; United States Attorney Bud Cummins for the Eastern District of Arkansas; United States Attorney R. Alexander Acosta for the Southern District of Florida; Steven D. Ricciardi, Special Agent in Charge of the U.S. Secret Service in New England; Kenneth W. Kaiser, Special Agent in Charge of the Federal Bureau of Investigation in New England; William Sims, Special Agent in Charge of the Secret Service in Miami, Florida; and William C. Temple, Special Agent in Charge of the Federal Bureau of Investigation in Little Rock, Arkansas, announced today that in a sealed court proceeding a Massachusetts teenager pled guilty before U.S. District Judge Rya W. Zobel to an Information charging him with nine counts of Juvenile Delinquency.

By statute, federal juvenile proceedings and the identity of juvenile defendants are underseal. The Court has authorized limited disclosure in this case at the request of the government and defendant.

Judge Zobel also imposed a sentence today of 11 months' detention in a juvenile facility, to be followed by 2 years of supervised release. During his periods of detention and supervised release, the Juvenile is also barred from possessing or using any computer, cell phone or other electronic equipment capable of accessing the Internet.

Had the Juvenile been an adult, the underlying charges would have been charged as three counts of Making Bomb Threats Against a Person or Property, three counts of Causing Damage

to a Protected Computer System, two counts of Wire Fraud, one count of Aggravated Identity Theft, and one count of Obtaining Information from a Protected Computer in Furtherance of a Criminal Act.

The Juvenile was also charged in an Information in the Eastern District of Arkansas with one count of Juvenile Delinquency. Had the Juvenile been an adult, the underlying charge in the Arkansas case would have been Causing Damage to a Protected Computer System. The case was transferred to the District of Massachusetts and the Juvenile pled guilty to the charge last month. Today's sentence is the result of the Juvenile's guilty plea to both the Massachusetts and Arkansas charges.

"Computer hacking is not fun and games. Hackers cause real harm to real victims as graphically illustrated in this case," stated U.S. Attorney Sullivan. "Would-be hackers, even juveniles when appropriate, should be put on notice that such criminal activity will not be tolerated and that stiff punishments await them if they are caught."

The basis for the charges was a course of criminal conduct that took place over a fifteen month period beginning in March, 2004 when the Juvenile sent an e-mail to a Florida school with the caption, "this is URGENT!!!". The text of the e-mail read:

> "your all going to perish and flourish...you will all die
> Tuesday, 12:00 p.m.
> we're going to have a "blast"
> hahahahahaha wonder where I'll be? youll all be destroyed. im sick of your **[expletive deleted]** school and piece of **[expletive deleted]** staff, your all gonna **[expletive deleted]** die you pieces of crap!!!!
> DIE MOTHER **[expletive deleted]** IM GONA BLOW ALL YOU UP AND MYSELF ALL YOU NAZI LOVING MEXICAN FAGGOT BITCHES ARE DEAD"

As a result of this bomb threat, the school was closed for two days, while a bomb squad, a canine team, the fire department and Emergency Medical Services were called in.

In August, 2004, the Juvenile logged into the Internet computer system of a major Internet Service Provider ("ISP") using a program he had installed on an employee's computer. This program allowed the juvenile to use the employee's computer remotely to access other computers on the internal network of the ISP and gain access to portions of the ISP's operational information.

In January, 2005, the Juvenile gained access to the internal computer system of a major telephone service provider that allowed him to look up account information of the telephone service provider's customers. He used this computer system to discover key information about an individual who had an account with the telephone service. He then accessed the information stored on this individual's mobile telephone, and posted the information on the Internet.

During this same time period, the Juvenile used his access to the telephone company's computer system to set-up numerous telephone accounts for himself and his friends, without having to pay for the accounts.

Also in January, 2005, an associate of the Juvenile set-up accounts for the Juvenile at a company which stores identity information concerning millions of individuals allowing the Juvenile to look at the identity information for numerous individuals, some of which he used for the purpose of looking up the account information for the victim whose personal information he posted on the Internet.

In the spring of 2005, the Juvenile, using a portable wireless Internet access device, arranged with one or more associates to place a bomb threat to a school in Massachusetts and local emergency services, requiring the response of several emergency response units to the school on two occasions and the school's evacuation on one.

In June, 2005, the Juvenile called a second major telephone service provider because a phone that a friend had fraudulently activated had been shut off. In a recorded telephone call, the Juvenile threatened the telephone service provider that if the provider did not provide him access to its computer system, he would cause its web service to collapse through a denial of service attack- an attack designed to ensure that a website is so flooded with request for information that legitimate users cannot access the website. The telephone service provider refused to provide the requested access. Approximately ten minutes after the threat was made, the Juvenile and others initiated a denial of service attack that succeeded in shutting down a significant portion of the telephone service provider's web operations.

The investigation of the Juvenile's associates is continuing.

The case was investigated by the U.S. Secret Service and the Federal Bureau of Investigation. The Massachusetts case was prosecuted by Assistant U.S. Attorneys Stephen Heymann and Seth Berman in Sullivan's Internet Crimes Unit. The Arkansas case was prosecuted by Assistant U.S. Attorney Karen Coleman in Cummins' Office. The prosecution in Florida was handled by Assistant U.S. Attorney Anita Gay in Acosta's Office.

Press Unit: Samantha Martin, (617) 748-3139